

IN THE CLAIMS

Claim 1 (Currently Amended): A system comprising:
a key generating section, the key generating section to generate a plurality of individual keys based on a main key, each of said plurality of individual keys is different from one another;
a decryption generating section coupled to the key generating section and a main decryption section, the decryption generating section to generate a plurality of individual decryption processes based on the main decryption section and the plurality of individual keys, each of said plurality of individual decryption processes is different from one another; and
a main encryption section, the main encryption section using the main key to encrypt content,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the main encryption section.

Claim 2 (Previously Presented): The system of claim 1, wherein each of the plurality of individual decryption processes each use a selected one of the plurality of individual keys.

Claim 3 (Previously Presented): The system of claim 2, wherein each of the plurality of individual decryption processes decrypt the content from cypher-content by using a selected one of the plurality of individual keys.

Claim 4 (Currently Amended): A circuit comprising:
a key generating section, the key generating section to generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another;

an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section to generate a plurality of individual encryption processes based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption processes being different from one another; and

a main decryption section, the main decryption section using the main key to decrypt cypher-content,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt content to be decrypted by the main decryption section.

Claim 5 (Previously Presented): The circuit of claim 4, wherein each of the plurality of individual encryption processes to each use one a selected one of the plurality of individual keys.

Claim 6 (Original): The circuit of claim 5, wherein each of the plurality of individual encryption processes encrypt the content forming the cypher-content by using the plurality of individual keys.

Claim 7 (Currently Amended): A method comprising:
generating a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another;
generating a plurality of individual decryption processes based on a main decryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and
encrypting content based on an encryption process and the main key,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the encryption process.

Claim 8 (Original): The method of claim 7, further comprising:
distributing the plurality of individual keys to a plurality of customers;
distributing the plurality of individual decryption processes to the plurality of customers; and
distributing cypher-content to the plurality of customers.

Claim 9 (Previously Presented): The method of claim 8, wherein each of the plurality of individual decryption processes to each use a selected one of the plurality of individual keys.

Claim 10 (Original): The method of claim 9, the encrypting to generate a cypher-content from the content.

Claim 11 (Previously Presented): The method of claim 10, wherein each of the plurality of individual decryption processes decrypt the content from the cypher-content by using a selected one of the plurality of individual keys.

Claim 12 (Currently Amended): A method comprising:
generating a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another;
generating a plurality of individual encryption processes based on a main encryption process and the plurality of individual keys, each of said plurality of individual encryption processes being different from one another; and
decrypting cypher-content based on a main decryption process and the main key,

wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cipher-content to be decrypted by the main decryption process.

Claim 13 (Original): The method of claim 12, further comprising:
distributing the plurality of individual keys to a plurality of customers;
distributing the plurality of individual encryption processes to the plurality of customers; and
receiving cypher-content from the plurality of customers.

Claim 14 (Previously Presented): The method of claim 12, wherein each of the plurality of individual encryption processes to each use a selected one of the plurality of individual keys.

Claim 15 (Original): The method of claim 12, the main decryption process to generate a content from the cypher-content.

Claim 16 (Previously Presented): The method of claim 15, wherein each of the plurality of individual encryption processes encrypt the content forming the cypher-content by using a selected one of the plurality of individual keys.

Claim 17 (Currently Amended): A program storage device readable by a machine comprising instructions that cause the machine to:

generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another;

generate a plurality of individual decryption processes based on a main decryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and

encrypt content based on an encryption process and the main key,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the encryption process.

Claim 18 (Original): The program storage device of claim 17, wherein the plurality of individual decryption processes to each use one of the plurality of individual keys.

Claim 19 (Original): The program storage device of claim 18, the encrypting to generate a cypher-content from the content.

Claim 20 (Previously Presented): The program storage device of claim 19, wherein each of the plurality of individual decryption processes decrypt the content from the cypher-content by using a selected one of the plurality of individual keys.

Claim 21 (Currently Amended): A program storage device readable by a machine comprising instructions that cause the machine to:

distribute a plurality of individual keys to a plurality of customers, each of said plurality of individual keys being different from one another;

distribute a plurality of individual decryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another; and

distribute cypher-content to the plurality of customers,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt cypher-content encrypted by a main encryption process.

Claim 22-23 (Canceled)

Claim 24 (Currently Amended): A program storage device readable by a machine comprising instructions that cause the machine to:

generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another;

generate a plurality of individual encryption processes based on a main encryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and

decrypt cypher-content based on a main decryption process and the main key,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cypher-content to be decrypted by the main decryption process.

Claim 25 (Canceled)

Claim 26 (Original): The program storage device of claim 24, the main decryption process to generate a content from the cypher-content.

Claim 27 (Previously Presented): The program storage device of claim 25, wherein the plurality of individual encryption processes encrypt the content forming the cypher-content by using a selected one of the plurality of individual keys.

Claim 28 (Currently Amended): A program storage device readable by a machine comprising instructions that cause the machine to:

distribute a plurality of individual keys to a plurality of customers, each of said plurality of individual keys being different from one another;

distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another; and

receive cypher-content from the plurality of customers,
wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cypher-content to be decrypted by a main decryption process.

Claim 29 (Canceled)

Claim 30 (Previously Presented): The program storage device of claim 29, wherein each of the plurality of individual encryption processes encrypt the content forming the cypher-content by using a selected one of the plurality of individual keys.